Soft Systems are Ubiquitous – Defenses are Rare: A Case for Contingent Outsourcing of Patch Management

Kirk P. Arnett
Mississippi State University

Abstract:
Computer attacks on vulnerable software are ubiquitous. Today's attacks on client PCs can be used to create armies of zombie computers that are capable of wide reach attacks on high profile businesses and governments. The simple act of patching software vulnerabilities will certainly mitigate this problem, but patching has its own set of problems. Further, it is frequently the case that patches which are available to mitigate vulnerabilities are not being made on a timely basis and sometimes are not being made at all. One solution to the patch management dilemma is outsourcing. This paper notes that outsourcing is not a carte blanche decision that can be made based on dollars, but rather that a contingency decision matrix can provide guidance on outsourcing solutions for patch management and other security components as well. The matrix recognizes that IS staff expertise and employee security awareness are two important factors in the outsourcing decision.

Key words:
outsourcing, security, patch management, vulnerabilities

1. Introduction

Most countries continually battle ever increasing computer attacks. These attacks on personal, business, and governmental computers present a worldwide problem so that worms such as the well known Sasser can reach 90% of unprotected hosts of the world's Internet connected SQL Servers in 10 minutes. The US has recent reports of the compromise of identity information for one-half of the current US Air Force officers. It is well known that North Korea trains hackers for cyber attacks against South Korean and others. One such facility, Kim il Sung's academy, conducts five years of specialty courses and graduates 100 hackers per year [4].

Although Korea and the US are separated by thousands of miles and have vastly different cultures, they have common Internet usage patterns. For instance, according to Internet World Stats [2] there is a 63.3% penetration of Internet users in Korea and a 68.5% penetration in the US. Both countries have roughly the same extent of, but rapidly expanding, broadband usage so there are large numbers of "always-on" Internet connections that can be attacked and placed in the Zombie armies.

Global hacker attacks represent a severe imbalance in that the defender must care for all vulnerabilities while the attacker needs only a single weak spot to win the battle. Some of these attacks, particularly those against governments by counties or non-governmental groups with political agendas, are referred to as cyber war and cyber terrorism, but in truth motivations other than war – money, fame, fun, disruption, etc. may be the driving force of these attacks. In fact money is said to be the driving force of the gangs of criminals who control the increasingly dangerous botnets. Given the imbalance between what the defender and attacker must do to win in these attack battles, a question that arises is to determine the best way to defend.

Conventional wisdom notes that security is a balancing act so that perfect security for an individual, company, or country will be unaffordable in terms of costs or impractical in terms of system usability. Many authorities believe that the greatest barrier to security effectiveness is an inadequate budget. Because of financial concerns and inadequate staff expertise on the defender side, outsourcing selected components of the security infrastructure to managed security service providers (MSSP) is often considered a winning strategy. Indeed, this paper supports outsourcing of select security components.

This paper examines a key component of security management; namely patch management, which exists for all computer users, and then suggests how to evaluate decisions regarding whether or not patch management should be outsourced. In the end, a view is held that outsourcing at least some security components must be a part of the security management solution. But the outsourcing decision must be made with three contingences in mind; namely 1) the security awareness and training of employees, 2) the expertise of the internal IS security staff, and 3) the specific component of the outsourcing being considered. To evaluate these contingencies, the classic categories of strategic relevance grid devised by Cash et. al [1] to evaluate management control strategies is reworked and revisited. This is done in the context of patch management, but the logic applies equally well for other security components such as firewall tuning, vulnerability tests, intrusion prevention, etc.

2. Security outsourcing

Outsourcing, or contracting with others to provide services which a company might otherwise have employed its own staff to perform, has been a viable option in manufacturing for organizations for many years. Most of the recommendations regarding outsourcing or offshoring suggest that cost savings are a key benefit.

Recently, there has been a surge of attention given to outsourcing and offshoring for computer services and in particular, computer security. Consider, for example, the question as to whether or not to outsource penetration testing. Although there is some belief that security should remain inside, this is a clear example where insiders present a problem. It makes little sense for a company to do its own penetration testing because of the pressure for inside testers to either overlook or secretly remedy any weak spots. Historically, cost savings and increased staff expertise are given as justification for outsourcing certain elements of security management. Beyond cost savings, one rationale is that people who specialize in work with a wide variety of security problems over time have a higher level of skill than do those who have experience with their own company. The parallel logic is that fire departments, because of their specialization in training and experience, will do a better job of fighting fire than internal staff of a company. Most would agree that some level of outsourcing is a smart business decision and there is abundant practitioner literature regarding how to write contracts and evaluate outsourcing partners. Also, most would agree that there are some security components that should not be outsourced. There are cautions against outsourcing core operations security components because outsiders will "know too much" about the company's business.

3. Patch management

Patches are pieces of software that are used to repair or work around vulnerabilities or weaknesses to another piece of software. Patches are perhaps best known in the Microsoft Windows arena where they are routinely released to allow users to protect their PCs from attack by patching "holes" in software such as Internet Explorer. Patches can be found for browsers, operating systems, web servers, database systems, or other software. Patches are routinely released by vendors, and this release occurs after the vendor, or others, has discovered the vulnerability. In the Unix-like world these patches may be installed via rpm, for instance in RedHat's Linux. Microsoft uses multiple methods to install patches in the Windows world. Some of these methods are when a shut down occurs, on a periodic basis, when the patch is available, etc., and these can be manually or automatically installed.

Patching is critical, but it is not used as frequently as should be. A mid-2002 survey of computer security professionals by IPSOS and reported by Panko [3] found that 57% of respondents even checked security bulletins at least once a week. And for personal computers the situation may even be worse. A recent SANS Institute poster notes that asking a computer user to patch a computer is no more effective than asking a driver not to drive faster than the limit. A major problem that leads to this situation is in the sheer number of patches that must be installed. For instance CERT counted 2148 vulnerabilities in the first half of 2002. And, in what has now become known as "patch Tuesday" Microsoft, Mozilla, Apple, Sun, and other vendors released numerous patches in July and again in August of 2005. The point is that the number of patches is too great and the frequency of patches is too often to be successfully managed by all computer owners and installations.

Installing patches also comes with some risks; one of which is reduced functionality. Some patches may freeze machines or do other damage. This explains why multiple patches are released in order to mitigate threats of a single vulnerability. A testing server is a way to examine the potential problems that may arise as a result of patch installation, but his is not practical with personal machines.

4. A context: BotNets

No longer are computer crimes subject to single computers or financial industry installations such as the well known salami slicing attacks. Now, in addition to Spyware and adware being unknowingly installed on the millions of PCs, legions of these computers have other malware installed so that they are "owned" by attackers, and these zombies or botnets are being used in coordinated attacks.

In a recent exploit of unpatched vulnerabilities, more than a dozen worms and variants were created to exploit a security hole in the plug-and-play feature in the Windows 2000 operating system. Oddly, according to Hypponen, some versions of the worm undo the effects of earlier worms, suggesting that the worm creators are battling to take over computers that have already been hacked [6].

These worms include "bot" code to allow the attacker control of a compromised computer from another location, and numbers of these computers are compromised into zombie botnets. Botnets are rented by criminal gangs to allow the renters to spam, phish, commit fraud, and launch denial of service attacks. Symantec notes that a botnet of 5,500 zombies costs spammers, phishers, etc. about $350 a week [6].

Botnets are easily created because of the large number of unpatched and always-on connected computers. Botnets are relatively cheap to the attacker as they can be rented or leased for a few cents per zombie computer. And, it will be some time before they are controlled because large ISPs cannot be shut down, botnets may use several different ISPs, and there is still a reluctance to scan email content at the ISP level. The ease with which these zombie botnets can be created is a direct result of the lack of knowledge or effort exerted by the employee in a business or governmental setting or the owner in a home setting. It follows then that education and awareness can be used to mitigate this problem. How do we prevent such problems? One way is to insure that the vulnerabilities which have been noted are patched as soon as vendor patches become available. But, this reactive stance may be too slow for flash viruses or zero-day exploits. However, help is on the way!

5. Promise for patches

Security vendors are helping fight the battle against botnets as more sophisticated approaches become available. According to Symantec [5] there is an average lag of 6.4 days between vulnerability announcement and patch availability. In the reactive mode, Symantec [5] can block signatures in four minutes, but still some viruses can spread before being blocked. Consider that companies not only have client PCs to manage but also host servers, the problem is even greater. Symantec uses generic exploit blocking where they code a patch management routine to protect the vulnerability rather than attempting to first understand the signature [5]. In this sense, one could argue that Symantec, an anti-virus solutions provider, is an outsourcing vendor or MSSP.

Certainly one of the most difficult, time-consuming, and even risky tasks for IT professionals is to maintain currency with patch management. This task requires IS personnel to be informed as to patch availability, decide how important patches are to the company, and if necessary deploy the patch with a minimum of potential conflicts. Products such as Symantec's LiveState™ Patch Manager provide assistance for this task. Regardless, there may be situations where it and/or other solutions are best handled by inside staff expertise. But, how should we evaluate these outsourcing decisions?

6. A case for contingency management:

Cash, McFarland, McKenney, and Vitale [1] introduced a four-quadrant grid of categories of strategic relevance to be used for management control. These categories are recast below as

Figure 1 with an axes representing skills and awareness of IS security staffs and employees. This grid can be used to aid decision makers as to whether or not to outsource a particular component of security. The context described below is for patch management, but the grid should work for the evaluation of other security components as well.

Quadrant I represents a company where employees have a high level of security awareness, but the internal security staff does not have a high level of skill. It is likely that this company can be managed without outsourcing. A possible strategy would be for top management of this company to craft a policy which states that all employees are to install patches on a twice-daily basis. Also a strong statement of belief of the importance of securing client PCs should be made. This visible top management support should be successful for client PCs in a QI company. The situation for host computers and their software may be quite different. If the skill and knowledge level is low, then the management might consider outsourcing of patch management for host machines as an immediate step. In addition, it is clear that more skills are needed by the professional staff, so additional training or skilled staff is needed.

Quadrant II exists where the company employees have a high level of awareness and its professional IS staff has high skill. In this case outsourcing of patch management does not seem to be appropriate. The reason is that enough skill exists in house among employees and security professionals to maintain patches on a timely basis. Also, the internal security staff can evaluate any negatives that might occur as a result of patch installation. For instance, is a host patch renders a piece of operable code to be inoperable, then the IS staff will be able to return to the pre-patch condition or they may have installed the patch on a staging server so that any negative effects will be determined before damage is done in production.

In the US, a security firm such as Symantec might be located in this quadrant. If there are outsourcing decisions, the internal staff expertise has likely already made them. Also, because of their expertise in the area, these decisions were made some time ago and there is little need to reevaluate them. If the particular outsourcing partner was inefficient or inappropriate or if other problems arose, then they were likely dealt with. The company will change vendors or tune contracts handle problems. So, although outsourcing might bring some efficiency through economies of scale house, effectiveness might decline.

A company that operates in Q III's lower left position of the figure is in imminent danger. The number of attackers and potential for attack is great as software vulnerabilities and exploits are a continuing certainty. The company can waste no time and must immediately acquire help via outsourcing. The relative expense may be greater for a small firm, but the potential for catastrophic failure is so great, that the decision here is one to insure survival. Further if the US figures are correct, most firms spend leas than 5% of the IT budget on security, so expense is not the key issue. Top managers of QIII companies must immediately seek professional help from outsiders. This help will be for patch management and for training. The training should be for both company employees and for IS.

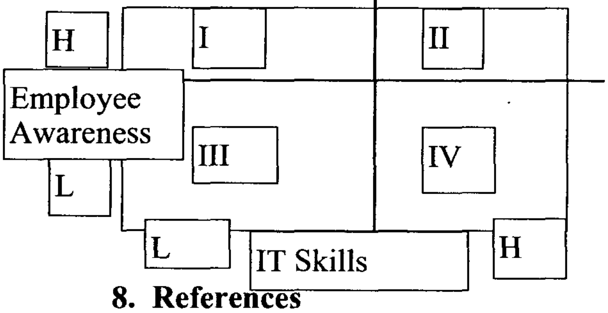
Quadrant IV presents yet another decision contingency. A company in QIV, despite the lack of awareness of its employees, might not need to seek outsourcing for patch management. Consider that there are basically two kinds of patching – one for hosts and another for client PCs. In the case of host computers, the IS security staff has a high level of expertise, so they stay abreast of security vulnerabilities and patches to them. Further, they have extensive knowledge about the local environment that is important to their applications' portfolio. For client PCs, there is a weakness in that the employees may not patch on a timely basis. But, the high level of skill of the IS security staff means that automated solutions have been created. So, they may be able to centrally control the settings of employee PCs and push appropriate patches to the clients when needed.

7. Decision maker implications

Software patching is a necessary inconvenience. It is necessary to protect host and client computers. Patching is inconvenient because it takes time from other productive or entertaining computing activities. There is ample evidence that patching is not performed as it should be. Some companies have the knowledge and experience to manage patches on their own. Others do not. The contingency matrix provides a means by which a decision maker can evaluate where his company lies, and then based on the strengths that exist for both employees and IS security staff, make a decision regarding how to protect the company's information assets. Hiring employees to accommodate low rankings in the matrix is a solution, but it is one that cannot work in the short term. The reason is that the new employees, whether security professionals or other staff, must also gain expertise of the company culture.

Outsourcing, where appropriate, provides an effective solution which can be implemented in the near term. Further, there are many situations when outsourcing may save money, but saving money is not the critical element of the security outsourcing decision. Effectiveness and quality of service are more important. The contingency matrix will aid the decision maker in deciding whether or not to outsource. But the decision maker must be fair in determining in which quadrant his company lies. Further, the matrix will work for security elements other than patch management, and should provide heightened security to all who use it.

Fig. 1 - Contingency Matrix



8. References

[1] JI Cash, Jr., FW McFarland, JL McKenney, and MR Vitale. (1988) Corporate Information Systems management: Text and Cases. Homewood, IL. Irwin.

[2] Internet World Stats (2005). http://www.internetworldstats.com

[3] Raymond R. Panko (2004) Corporate Computer and Network Security. Pearson, Prentice-Hall Upper Saddle River, NJ.

[4] Pravda (2004). North Korean hackers sabotage computer networks of South Korea. http://english.pravda.ru/world/20/91/366/14396_nkorea.html October 7, 2004.

[5] Symantec Corporation (2005). Webcast August 18, 2005.

[6] David Quainton (2005). "Windows vulnerability sparks viral warfare." SC Magazine, August 2005. http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=41586e4a-5db7-41ae-9f39-4538d93505af&newsType=News

Dr. Kirk P. Arnett is a professor of information systems in the Management & Information Systems Department of Mississippi State University's College of Business & Industry. He is a Certified Computing Professional and is certified in Global Security Essentials. He has received the College of Business Outstanding Research Award and outstanding Faculty Member Award. He is a member of AIS, ACM and AITP.